

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization International Bureau



(43) International Publication Date
5 February 2004 (05.02.2004)

PCT

(10) International Publication Number
WO 2004/012415 A1

(51) International Patent Classification⁷: H04L 29/06, 12/58, G06F 1/00

(74) Agents: EXELL, Jonathan et al.; Morley House, 26-30 Holborn Viaduct, London EC1A 2BP (GB).

(21) International Application Number: PCT/GB2003/003243

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(22) International Filing Date: 21 July 2003 (21.07.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0217610.5 30 July 2002 (30.07.2002) GB
03250672.7 3 February 2003 (03.02.2003) EP

(71) Applicant (for all designated States except US): SECURITY AND STANDARDS LIMITED [GB/GB]; Suite A, 192 Moulsham Street, Chelmsford, Essex CM2 0LG (GB).

(72) Inventors; and

(75) Inventors/Applicants (for US only): POPE, Nicholas, Henry [GB/GB]; 167 Mountnessing Road, Billericay CM12 0EE (GB). ROSS, John, Gordon [GB/GB]; 38 Quilp Drive, Chelmsford CM1 4YA (GB).

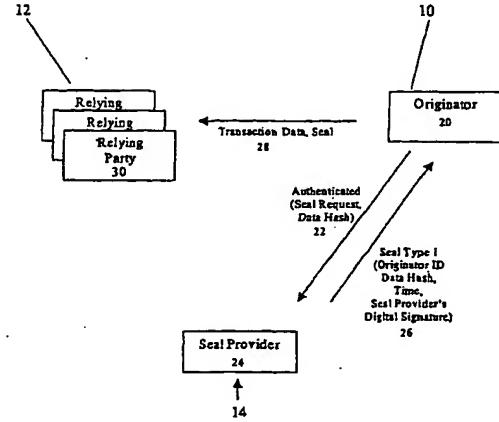
(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

- with international search report
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

[Continued on next page]

(54) Title: ELECTRONIC SEALING FOR ELECTRONIC TRANSACTIONS



WO 2004/012415 A1

(57) Abstract: A sealing method and system based on any data originator authentication mechanism involves an originator (10) which represents the entity requiring the data to be sealed and to have itself identified as the originator of the sealed data. The relying party (12) is an entity requiring to use the sealed data as proof relating to a transaction. The seal provider (14) is an entity trusted to provide seals by the originator and relying parties. The procedure for creating a seal is as follows: the originator (10) creates a hash value or other one-way representation of the data to be sealed. The originator (10) then sends the hash value with a seal request through a secure channel which authenticates the originator (10) to the seal provider (14) and ensures the integrity of the request. The seal provider (14) then determines if the authentication of the request is correct and, if so, creates a seal which contains an identifier for the originator (10), the time of the request, the hash value and a digital signature or other similar mechanism which authenticates the data unit as coming from the seal provider (14). The preferred form of digital signature is one using public key cryptography such as specified in ITU-T X.509 or Internet RFC 2560.



For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

ELECTRONIC SEALING FOR ELECTRONIC TRANSACTIONS

The present invention relates to an electronic sealing method and to an electronic registration method for use in electronic transactions.

Existing electronic signature methods are commonly based on use of public/private key (asymmetric) cryptography to create a digital signature supported by electronic certificates (e.g. as defined in ITU-T X.509). This requires use of certificate status methods such as Certificate Revocation Lists (as defined in ITU-T X.509) or on-line certificate status checking (as defined in Internet RFC 2560) to ensure the validity of certified key (revoked or not). As the validity of the certified key used to create a digital signature may change over time, it is often considered necessary to know the time at which the signature was created. This can be achieved by applying a secure time-stamp method (Internet RFC 3161, US patent RE 34,954) over the digital signature (ETSI TS 101 733).

Secure time-stamping methods (Internet RFC 3161; US patent RE 34,954) can also be used on their own (without the digital signature of the originator) to provide integrity of transaction data and proof of transaction time. This does not, however, provide any proof of the originator.

These electronic signature methods have two major disadvantages. First, it can be difficult to gain assurance of the validity of the public key used to verify the digital signature (that is the signature verification key). When verifying a signature the relying party needs to obtain information on the status of certificate used to validate the signing key. This can involve a significant overhead in obtaining the appropriate (revocation) status information. It can be particularly difficult, if not impossible, to get this status information as it applied when the signature was created when there is a significant period between the creation of the signature and its verification (as in the case of a subsequent dispute over a transaction).

Secondly, the certificate, which relates a name to a signing key, is often created by a party which is not directly involved with the business using that certificate. As the subject of the certificate is not already "known" to the authority issuing the certificate (the

certification authority), there can be difficulty in checking the subject's name. This can result in significant additional costs and also increases the probability of errors.

5 The present invention seeks to provide an electronic sealing and an electronic registration method for use in electronic transactions.

According to an aspect of the present invention, there is provided a sealing method for sealing the details of an electronic transaction including the step of obtaining authentication information from an originator, checking the validity of that originator's 10 authentication at the time of the transaction and creating a sealed record related to the transaction and validity of the originator's authentication information.

15 Preferably, the sealed record includes details of the originator of transaction data and the time of the transaction and thereby proves the integrity of the transaction data. The seal is preferably digitally signed by a trusted seal provider. In the preferred embodiment, the transaction data itself is not revealed to the seal provider enhancing its confidentiality. The seal may include other information relating to a transaction originator such as a copy 20 of originator's public key certified by the seal provider.

25 The method advantageously forms an electronic signature having non-repudiation properties. The method may use any data originator authentication mechanism or more specific form of originator authentication using digital signatures based on public key cryptography.

30 The preferred sealing method overcomes the first disadvantage mentioned above by checking the validity of originator's authentication information (for example signing key) at the time of the transaction. The registration method overcomes the second disadvantage mentioned above by involving a party involved in the business functions in the registration process.

According to a preferred embodiment of the present invention. The method includes the steps of:

the originator digitally signing a transaction data or other data,
transmitting the transaction data or other data or a hash value or another
representation of the transaction, the digital signature and a seal request to the or a seal
provider;

5 providing for the seal provider to determine whether the authentication of the
request is correct and whether the digital signature is currently valid and if so creating a
seal.

10 The seal may contain an identifier for the originator, the time of the request, the
transaction data or other data, hash value or other one-way representation, by the
originator, and at least one digital signature or other authentication of the seal as coming
from the seal provider. The seal may also contain a digital signature provided by the
originator which has been checked by the seal provider.

15 The originator may be a transaction peer. The sealed record may include a text
header and binary data encoded as a text string.

20 The method may preferably further comprise the step of encoding the transaction
data or other data and the sealed record, the encoding being arranged such that upon
accessing the encoded data, the sealed record is displayed in a first area of a computer
interface and the transaction data or other data is displayed in one or more other areas.
The encoding may comprise MIME and HTML encoding and the areas comprise
frames.

25 According to another aspect of the present invention, there is provided a computer
implemented transaction method comprising the steps of accepting one or more user inputs
specifying a transaction, submitting authentication data and data representative of
transaction data to a system operating the method of any of the preceding claims for
creating a sealed record, receiving said sealed record and storing said sealed record and at
30 least selected parts of said data representative of transaction data or the transaction data.

According to another aspect of the present invention, there is provided a system for providing a seal for sealing the details of an electronic transaction or data including means for obtaining authentication information from an originator, means for checking the validity of that originator's authentication at the time of sealing and means for creating a sealed record related to the transaction or data and validity of the originator's authentication information.

According to another aspect of the present invention, there is provided a transaction system arranged to accept one or more user inputs specifying a transaction, submit authentication data and data representative of transaction data to a system for creating a sealed record as defined above, receive said sealed record and store said sealed record and at least selected parts of said data representative of transaction data or the transaction data.

Preferably the system further comprises a client interface, the transaction system being arranged to transmit said sealed record and said at least selected parts of said data representative of transaction data or the transaction data to the client interface.

Preferably, the system further comprises a validation interface, the validation interface being arranged to accept a user input to validate an existing sealed record, the validation interface being operative to transmit said sealed record and said data representative of transaction data to a validation system for validating said sealed record, said validation system being arranged to generate at least part of a sealed record, compare it to said sealed record and output a result of said comparison to said validation interface.

25 The system may comprise one or more web pages.

In one embodiment, an email system may incorporate or interface with a transaction system as defined above. The email system may be arranged to receive an email message for an intended addressee, submit data from said email or data representative of data from said email to the system to obtain a sealed record, append the sealed record to the email message and transmit the email message and appended sealed record to the intended addressee.

The invention also seeks to provide a sealing method for sealing the details of an electronic transaction or data including the step of obtaining authentication information from an originator, obtaining an identification of the originator at the time of sealing and 5 creating a sealed record related to the transaction or data and validity of the originator's identification.

In the preferred embodiment, a one-way mathematical function of the transaction data, and not the data itself, is revealed to the seal provider. This may be used to ensure 10 that the seal applies to the data in its original form.

Embodiments of the present invention are described below, by way of example only, with reference to the accompanying drawings, in which:

15 Figure 1 shows an embodiment of sealing method using any originator authentication mechanism;

Figure 2a shows an embodiment of sealing method based on originator digital signatures;

20 Figure 2b shows an embodiment of sealing method incorporating a certified copy of the originator's public key;

Figure 3 shows an embodiment of sealing method for email transactions;

25 Figure 4 shows an embodiment of sealing method providing a transaction peer;

Figure 5 shows a modification to the embodiment of sealing method of Figure 4;

30 Figure 6 shows an embodiment of sealed registration method and in particular an originator set-up stage;

Figure 7 shows the steps of a routine for creating a sealed registration document;

Figure 8 shows a example of how a sealed document may be encoded as a text string;

5

Figure 9 shows a example of how a sealed document may be displayed; and

Figure 10 shows the steps of how a trusted agent may be used to validate a seal.

10 Referring to Figure 1, there is shown an embodiment of sealing method which is based on any data originator authentication mechanism. The scenario depicted in Figure 1 involves an originator 10 which represents the entity requiring the data to be sealed and to have itself identified as the originator of the sealed data. The relying party 12 (of which there may be more than one) is an entity requiring to use the sealed data as proof relating to 15 a transaction. This may, for example, include the recipient of the transaction data, an arbitrator or judge in a dispute or even the originator.

20 The seal provider 14 is an entity trusted to provide seals by the originator and relying parties. The seal provider 14 can be a system operated by any suitable organisation, such a business specialising in the provision of security services, trade organisation or any other suitable organisation.

25 In this embodiment and scenario depicted in Figure 1, the procedure for creating a seal is as follows. In the first instance, at step 20, the originator 10 creates a hash value (for example, the secure hash algorithm SHA1 defined in FIPS 180-1) or other one-way representation of the data to be sealed (typically the transaction data). At step 22 the originator 10 sends the hash value with a seal request through a secure channel which authenticates the originator 10 to the seal provider 14 and ensures the integrity of the request.

30

At step 24, the seal provider determines if the authentication and integrity of the request are correct. If so, the seal provider 14 creates a data unit, conveniently referred to

in this description as a seal, which, in this embodiment, contains an identifier for the originator 10, the time of the request, the hash value and a digital signature or other similar mechanism which authenticates the data unit as coming from the seal provider 14. The preferred form of digital signature is one using public key cryptography such as specified. 5 in ITU-T X.509 or Internet RFC 2560. The seal provider 14 may also copy the data forming the seal into an audit log file to provide an additional mechanism for assuring the validity of the transaction.

At step 26, the seal is returned to the originator 10. At step 28, the transaction data 10 with its seal is passed to each relying party 12, either directly or indirectly.

At step 30, any relying party 12 which trusts the seal provider 14 can verify the seal and the integrity of the transaction data to which the seal is applied by verifying the digital signature in the seal. Thus, the relying party 12 is provided with proof of the originator of 15 the transaction data, the time of transaction and the integrity of the transaction data.

Figure 2 shows an embodiment of sealing method which is based on a digital signature from the originator and still provides the scenario of one originator 10, one or 20 more relying parties 12 and a seal provider 14.

In this scenario, the preferred procedure for creating a seal involves the following steps. At step 40 the originator 10 digitally signs a transaction data and creates a hash 25 value or other one-way representation of that transaction data. At step 42 the originator 10 sends the hash value and the digital signature(s), with a seal request, through a secure channel which authenticates the originator 10 to the seal provider 14 and ensures the integrity of the request. In this embodiment, the request need not necessarily be 30 authenticated. If the request is not authenticated, the digital signature is used to authenticate the originator 10. Other parties may later submit the signed data for sealing but the seal with the earliest time can be taken as the one representing the time of the original transaction.

At step 44 the seal provider 14 determines whether the authentication and integrity of the request is correct and also whether the digital signature is currently valid, using the signature verification key of the originator 10. If this is the case, the seal provider 14 creates a data unit called a seal which, in this example, contains: an identifier for the 5 originator 10, the time of the request, the hash value, the digital signature provided by the originator 10, and at least one digital signature or other similar mechanism which authenticates the data unit as coming from the seal provider 14. The seal provider 14 may also copy the data forming the seal into an audit log file to provide an additional mechanism of assuring the validity of the transaction.

10

At step 46 the seal is returned to the originator 10. At step 48 the transaction data with its seal is passed to each relying party 12.

At step 50, any relying party 12 which trusts the seal provider 14 can verify the seal 15 and the integrity of the transaction data to which the seal is applied by verifying the digital signature(s) in the seal. Thus, each relying party 12 is provided with proof of the originator 10 of the transaction data, the time of transaction, the integrity of the transaction data and the validity of the digital signature which the originator 10 applied to the transaction data at that given time. In this embodiment, as is depicted in Figure 2a, two 20 digital signatures may be provided, the originator's digital signature and the seal provider's digital signature.

A variation for the sealing method based on digital signatures, as shown in Figure 2b, is one providing a public key that is certified by the sealing authority as being valid at 25 the time of the transaction. In this variation, the originator 10 includes a request for its public key be certified in the seal request 42b to the seal provider 14. The seal provider checks that the originator's public key is valid 44b, for example by checking the validity period in the originator's current X.509 identity certificate and the revocation status of that certificate. If the originator's public key is valid then this is included in the seal certifying 30 the validity of the key at the time of the transaction 46b. The originator sends this seal along with the digital signature to the relying party 48b. The relying party verifies the

digital signature using the public key in the seal 50b that the sealing authority certifies as being valid at the time of the transaction.

This form of seal (i.e. one including the public key) may be used as an alternative a 5 public key certificate (such as defined in X.509) with the validity only for a specific transaction (i.e. a transaction certificate). Furthermore, a seal may be used as a "qualified certificate" meeting the requirements identified in the European Directive 1999/93/EC on a "Community framework for electronic signatures" as described in the following table.

EU Electronic Signature Directive 1999/93/EC – Annex I Requirement on Qualified Certificate Content	Qualified Seal
(a) an indication that the certificate is issued as a qualified certificate;	Additional transaction attribute indicating that the seal is a form of qualified certificate;
(b) the identification of the certification-service-provider and the State in which it is established;	Already identified through the Sealing Authority certificate. This could be repeated as in an additional transaction attribute.
(c) the name of the signatory or a pseudonym, which shall be identified as such;	Already included in user name.
(d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;	Additional transaction attribute
(e) signature-verification data which correspond to signature-creation data under the control of the signatory;	Additional transaction attribute containing user public key

(f) an indication of the beginning and end of the period of validity of the certificate;	Validity period is for a single transaction at the time already given in the time-stamp.
(g) the identity code of the certificate;	Already in time-stamp serial number
(h) the advanced electronic signature of the certification-service-provider issuing it;	Already in the time-stamp signature
(i) limitations on the scope of use of the certificate, if applicable; and	Additional transaction attribute
(j) limits on the value of transactions for which the certificate can be used, if applicable.	Additional transaction attribute

This further enhanced seal, which is called herein a "qualified seal", has additional advantages over an X.509 based certificate in that:

- 1) This qualified seal may be used to provide an electronic signature that under 5 the European Directive 1999/93/EC article 5.1 "satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper-based data".
- 2) A user who already has conventional X.509 certificate, which does not meet the above legal requirements, can use that certificate to obtain a "qualified seal", which 10 does meet these requirements.
- 3) As the "qualified seal" is valid only for a particular transaction uncertainty over the validity of the certificate as the time of the transaction is minimised.
- 4) As the "qualified seal" applies to a single transaction the issuing authority has much greater control over its liability.

A variation to the sealing methods described above with respect to Figures 1, 2a and 2b is shown in Figure 3 and, in this example, relates to email transaction environments.

As illustrated in Figure 3, a seal request is passed to the seal provider 14 at step 60, which is then to be subsequently forwarded to the recipient(s) 12 identified in the recipient list. The transaction data is passed to the seal provider 14 together with the seal request and then is forwarded, at step 62, with the resulting seal to the identified recipient(s) 12.

5

Figure 4 shows another scenario of sealing method for use with transaction peers. As illustrated in Figure 4, at step 70 a seal request from the originator 10 is passed through the peer 15 with whom the originator 10 is carrying out the transaction. The seal request is passed, at step 72, to the seal provider 14 only if the transaction peer 15 agrees with the 10 transaction. At step 74 the seal is returned by the seal provider 14 to the transaction peer 15 and subsequently, at step 76, passed to the originator 10.

Figure 5 shows another scenario of sealing method for with transaction passing through the seal provider. As illustrated in Figure 5, at step 80 references to the originator 15 and transaction data (for example a universal Resource Identifier, see Internet RFC 2396) is passed from the originator 10 to the transaction peer 15. The preferred form of the reference to the transaction data is that the reference value is unpredictable, to avoid unauthorised access to the transaction data. The transaction peer 15 then sends these references to the seal provider 14 at step 82. The seal provider 14 then requests the 20 transaction data from the originator 10 at step 84, which returns with the transaction data through a secure channel which authenticates the originator 10 at step 86. The seal provider 14 then creates the seal which it passes, along with the transaction data, to the transaction peer 15 at step 88. The seal may also be sent back to the originator 10, with the reference to the transaction data, at step 90.

25

The preferred embodiments of seal registration methods provide two forms of identification, the first being a security system identifier and the second being a business identifier.

30

The preferred seal registration method is a technique for securely binding a security system identifier to a business identifier.

The security system identifier is allocated and authenticated by a security system, such as one of the implementations of sealing method described above. When allocated, this identifier is unrelated to any "real world" identification but can be used with a security system for identification purposes. A security system identifier may, for example, be a

5 number pair allocated by a seal provider 14 to an originator of sealed data. One number of the number pair identifies a community of users, the other number identifies the user within the community. The number pair is unique within the set of identifiers allocated by the seal provider.

10 The business identifier provides a set of attributes used by the business to identify an entity (such as a customer) for the purposes of transacting business therewith. This may include, for example, references used within the business (such as a customer reference number) and/or information used to identify the entity more generally (such as the customer's name and home address). The business identifier is agreed between the subject

15 and a registration authority. Some attributes may be allocated by the registration authority (for example, customer number), others may be provided by the subject (for example, first name, surname and address). The registration would either be a system operated by or on behalf of the business with which the subject is trading, or the registration authority would be operated by a third party business whose function is to check information concerning

20 the user.

When being set up to use one of the sealing methods described above, a sealed data originator 21 is allocated a security system identifier by a seal provider 14, as shown in Figure 6. Before allocating a security system to the originator identifier, the seal provider proves ownership of some means for authentication. In the embodiment using public key techniques this involves proof of possession of a private signing key.

Having set up two seal originators 21 which are to be parties in a business transaction, such as a business and its customer, a sealed registration document is created.

30 One party (for example the business) acts as a registration authority for the other party (for example, the customer). The customer acts as a subject of the registration. Between them,

these two parties create a sealed registration document which binds the subject identifier to the business identifier.

5 In the preferred embodiment, the sealed registration document is allocated a document reference (for example a Universal Resource Identifier, see Internet RFC 2396) by the registration authority. This registration document reference can later be used in subsequent sealed documents produced by the subject, thereby providing reference to its authenticated business identifier.

10 In the preferred embodiment, the sealed registration document contains:

- (a) the business identifier,
- (b) the registration document reference or some other information that may be used to identify the registration for a particular business purpose,
- (c) a seal from the subject which includes its security system identifier and

15 which indicates the subject's agreement that the business identifier is correct for itself,

- (d) a seal from the registration authority which indicates the registration authority's agreement that the business identifier is correct for the subject which created the seal in step (c) above.

20 An embodiment of routine for creating such a sealed registration document between a business acting as the registration authority and a customer acting as a subject of the registration is shown in Figure 7.

25 The procedure of the example of Figure 7 is as follows. At step 100, the subject 17 and the registration authority 19 establish the attributes required for the business identifier of the subject 17, such as name, address, customer identifier and so on.

30 At step 102, the registration authority 19 allocates the registration a reference (for example a Universal Resource Identifier) which is sent to the subject 17. At step 104, the subject 17 sends to the registration authority 19 a sealed document containing the business identifier and the registration document reference. The seal indicates the entity identified

with the security system identifier in the seal and agrees that the business identifier is applicable to itself.

At step 106, if the registration authority 19 has also agreed that the business identifier is applicable to the subject 17 which sent the sealed document, it will add its own seal. This sealed registration document is stored by the registration authority 19 and, if required, also passed to the subject 17 for later use in verifying a claim of identity.

Any sealed document can then include the appropriate registration reference to authenticate the identity of the originator.

The business operating as a registration authority 19 may similarly obtain a sealed registration with the seal provider 14 which, in turn, acts as another registration authority for the business registration authority.

15

It will be appreciated that the various embodiments described above can be combined with one another, as required in any particular implementation of the systems described herein.

20 It will also be appreciated that the embodiments described can provide a method of sealing data by a trusted third party to provide independent proof of: the originator, of the transaction data, the time of transaction, and the transaction data. The sealing method produces a form of electronic signature, which has non-repudiation properties and avoids the need for certificate revocation or other authentication status checking. The preferred 25 sealing method builds on existing secure time-stamping methods.

30 A method of encoding a seal provides a text string containing a descriptive header and binary protection data encoded in Base64 as defined in Internet RFC 2045. The header includes information on: the identity of the sealing authority, the originator's identity (system security identity and business identity) and the time of the transaction. The binary protection data includes binary encoding of the sealing authorities digital signature against a hash of the transaction data with the originator's identity and the time of the transaction.

An example of a text string encoding is given in Figure 8. An alternative encoding is to encode the data as described above in XML as defined in World Wide Web Consortium (W3C) specification Extensible Markup Language (XML) (reference <http://www.w3.org/TR/REC-xml>).

5

A method of encoding the transaction data with the seal uses the encoding defined in Internet RFC 2045 to RFC 2049 (commonly called MIME) combined with code for viewing hypertext in multiple frames such as defined in the World Wide Web Consortium (W3C) HTML 4.01 Specification (reference: <http://www.w3.org/TR/html4/>). The seal 10 itself, encoded as described above, is shown in one frame as a text string, only the header need be immediately visible. The sealed document is in the other frame or frames. This enables sealed documents, including documents incorporating text, images, voice or video, to be viewed through any suitably MIME enabled Web Browser. An example of a sealed document is given in Figure 9.

15

Referring to Figure 10, an embodiment of routine illustrating how a trusted agent may be used to validate a seal is shown. At step 120 the seal provider 14 issues a seal to the originator 10, which in turn, at step 122, provides the data and seal to the relying party 12. At step 124 the relying party 12 forwards the hash of the data together with the seal to 20 a seal validator 23 which, at step 125, determines whether the seal is valid. At step 126 the seal validator 23 returns to the relying party 12 a valid/invalid reply.

The embodiments described above provide a number of features for the creation of 25 a secure seal for subsequent use. First, the seal protects the authenticity of a data such as a document or transaction. This protection applies to the data both when communicated between systems and in storage. The seal can be applied to a hash of data along with the time and authenticated identity of the data originator. The authenticity is certified using, for example, the digital signature of the seal provider.

30 The seal provides long term authenticity of the data and in a form which cannot be repudiated, for example by claiming compromise of authentication keys subsequent to the seal being applied. Thus, a seal is provided which establishes the authenticity of the

parties and seals the transaction data in a manner which maintains its integrity over time. A copy of the seal can be kept by the seal provider in an audit log to provide further proof of authenticity. As the seal only contains a hash of the data being sealed, from which the original data cannot be re-created, the privacy of the data is maintained.

5

The seal can be used by the originator and any other party relying on the authenticity of data to validate its authenticity. Any party that trusts the seal provider and has a means of authenticating the seal (e.g. using the seal providers public key) can verify the validity of the seal. The hash value within the seal can be checked against a 10 recalculated hash value to check that the seal applies to the given data and that the data has been unchanged. Further assurance of the validity of a seal can be achieved by requesting a copy of the seal from the seal provider's audit log.

In this embodiment, once a transaction record and receipt (seal) has been generated, 15 as well as the seal to the appropriate party, a copy is saved at the seal provider or at a secure location controlled by the seal provider.

In some embodiments, such as those involving a transaction sequence a seal can be applied to each stage of the transaction proving the timing sequence of the transactions. 20 For example, in a transaction involving an offer and an acceptance, data relating to the offer and also to the acceptance can be each be sealed proving the time relationship between the offer and acceptance. This can, for example, have particular application in trading in shares.

25 It is also envisaged that in some embodiments the generation of the seal also stores data relating to a single event. For example, the event might be the creation of documents or data by an identified originator at a given time. The seal, therefore, would provide evidence of that event.

30 Thus, in the preferred embodiments, the seal is issued by a trusted authority (the seal provider) which authenticates the document originator, provides proof of time of creation of the document linked to a hash code representing the document and is protected

by a cryptographic code which proves the authenticity of the seal and which can detect any changes in the sealed information. The seal, along with the data it authenticates, can be sent to any party relying on the authenticity of that data.

5 In this regard, a seal can be checked for validity by the relying party or an agent trusted by the relying party to validate seals (seal validator). As shown in figure 10, the trusted agent can be used to validate a seal simply by forwarding the seal and a recalculated hash of the data to that party (124). This can be initiated, for example, by the relying party clicking on a button or icon displayed as part of the seal. If the seal validator 10 knows and trusts the sealing authority and has the key necessary to verify the cryptographic code (e.g. the sealing authority's public key) it can check the validity of the seal and confirm that the hash in the seal matches that recalculated by the relying party. If the seal is valid and the data hash is the same, the validator would respond by indicating that the sealed document provided by the relying party is valid (126). On the other hand, if 15 there has been any change in the seal, the cryptographic code was not created a trusted sealing authority or the hash in the seal does not match the recalculated hash, the seal provider would indicate that that seal has become invalid.

20 Thus, the preferred embodiment can provide a seal which is a form of certificate, specific to each transaction which incorporates attributes. This seal certifies the user's signing key, as well as providing a time stamp for relating to the transaction or event. This seal provides a form of certificate which is bound to the transaction, i.e. is transaction specific.

25 The seals can also be used for voice and video data and indeed can be applied to any digitised media such as web pages, video files, audio files, digital photographs and so on. In the preferred embodiment, the seals are simple to view and verify using, for example, an Internet browsing software. Furthermore, the seals can enable disputes to be resolved quickly, saving time and money. It can also protect all parties against denial of 30 the existence or content of a document or event and can provide evidence of a transaction or data when the information is contested, even years after the event.

Three variations of the sealing method have been described, one using originator authentication, the second adding originator digital signatures, the third adding public keys certified to be valid at the time of the transaction. Further variations of the sealing methods are envisaged for alternative transaction environments including but not limited to 5 e-mail, requests passed via transaction peers and transaction data passing through the seal provider.

There is also described a method for registration that applies the sealing method to the registration of a business identity between business partners. The registration method 10 can be used as an alternative to existing electronic certification methods. The registration method enables alternative business related registrations to be applied to the same entity for different business applications.

CLAIMS

1. A sealing method for sealing the details of an electronic transaction or data including the step of obtaining authentication information from an originator, checking the validity of that originator's authentication at the time of sealing and creating a sealed record related to the transaction or data and validity of the originator's authentication information.
- 10 2. A method according to claim 1, wherein the sealed record includes details of the originator of the transaction or data and the time of sealing.
- 15 3. A method according to claim 1 or 2, including the step of digitally signing the seal.
4. A method according to claim 3, wherein the step of digitally signing the seal is carried out by a trusted seal provider.
5. A method according to claim 4, wherein the transaction data or other data itself is not revealed to the seal provider.
- 20 6. A method according to any preceding claim, wherein a result of a one-way mathematical function applied to the data, is revealed to the seal provider.
- 25 7. A method according to any preceding claim, including the step of storing a copy of the data forming the seal into an audit log file held remotely from parties to the transaction or involved in the data.
- 30 8. A method according to any preceding claim, wherein the seal is passed to a relying party directly or indirectly.

9. A method according to any preceding claim, including the step of providing for checking of a seal, and that it belongs to data which is identical to that to which the seal was originally applied, by a relying party or an agent trusted by the relying party.

5 10. A method according to any preceding claim, including the steps of:
the originator digitally signing a transaction data or other data,
transmitting the transaction data or other data or a hash value or another
representation of the transaction, the digital signature and a seal request to the or a seal
provider;

10 providing for the seal provider to determine whether the authentication of the
request is correct and whether the digital signature is currently valid and if so creating a
seal.

11. A method according to claim 10, wherein the seal contains: an identifier for
15 the originator, the time of the request, the transaction data or other data, hash value or other
one-way representation, by the originator, and at least one digital signature or other
authentication of the seal as coming from the seal provider.

12. A method according to claim 11, wherein the seal also contains a digital
20 signature provided by the originator which has been checked by the seal provider.

13. A method according to any preceding claim, wherein the originator is a
transaction peer.

25 14. A method according to claim 13, wherein the sealed record includes a text
header and binary data encoded as a text string.

15. A method according to any preceding claim, further comprising the step of
encoding the transaction data or other data and the sealed record, the encoding being
30 arranged such that upon accessing the encoded data, the sealed record is displayed in a first
area of a computer interface and the transaction data or other data is displayed in one or
more other areas.

16. A method as claimed in claim 15, wherein the encoding comprises MIME and HTML encoding and the areas comprise frames.

5 17. A computer implemented transaction method comprising the steps of accepting one or more user inputs specifying a transaction, submitting authentication data and data representative of transaction data to a system operating the method of any of the preceding claims for creating a sealed record, receiving said sealed record and storing said sealed record and at least selected parts of said data representative of transaction data or
10 the transaction data.

18. A computer program comprising computer program code means for performing all of the steps of any of claims 1 to 17 when said program is run on a computer.

15

19. A computer program as claimed in claim 18 embodied on a computer readable medium.

20. A system for providing a seal for sealing the details of an electronic transaction or data including means for obtaining authentication information from an originator (10), means for checking the validity of that originator's authentication at the time of sealing and means for creating a sealed record related to the transaction or data and validity of the originator's authentication information.

25 21. A transaction system arranged to accept one or more user inputs specifying a transaction, submit authentication data and data representative of transaction data to a system for creating a sealed record according to claim 20, receive said sealed record and store said sealed record and at least selected parts of said data representative of transaction data or the transaction data.

30

22. A transaction system according to claim 21, further comprising a client interface, the transaction system being arranged to transmit said sealed record and said at

least selected parts of said data representative of transaction data or the transaction data to the client interface.

23. A transaction system according to claim 21 or 22, further comprising a
5 validation interface, the validation interface being arranged to accept a user input to validate an existing sealed record, the validation interface being operative to transmit said sealed record and said data representative of transaction data to a validation system for validating said sealed record, said validation system being arranged to generate at least part of a sealed record, compare it to said sealed record and output a result of said comparison
10 to said validation interface.

24. A transaction system according to any of claims 21 to 23 comprising one or more web pages.

15 25. An email system including a system according to any of claims 20 to 24, the email system being arranged to receive an email message for an intended addressee, submit data from said email or data representative of data from said email to the system to obtain a sealed record, append the sealed record to the email message and transmit the email message and appended sealed record to the intended addressee.

1/11

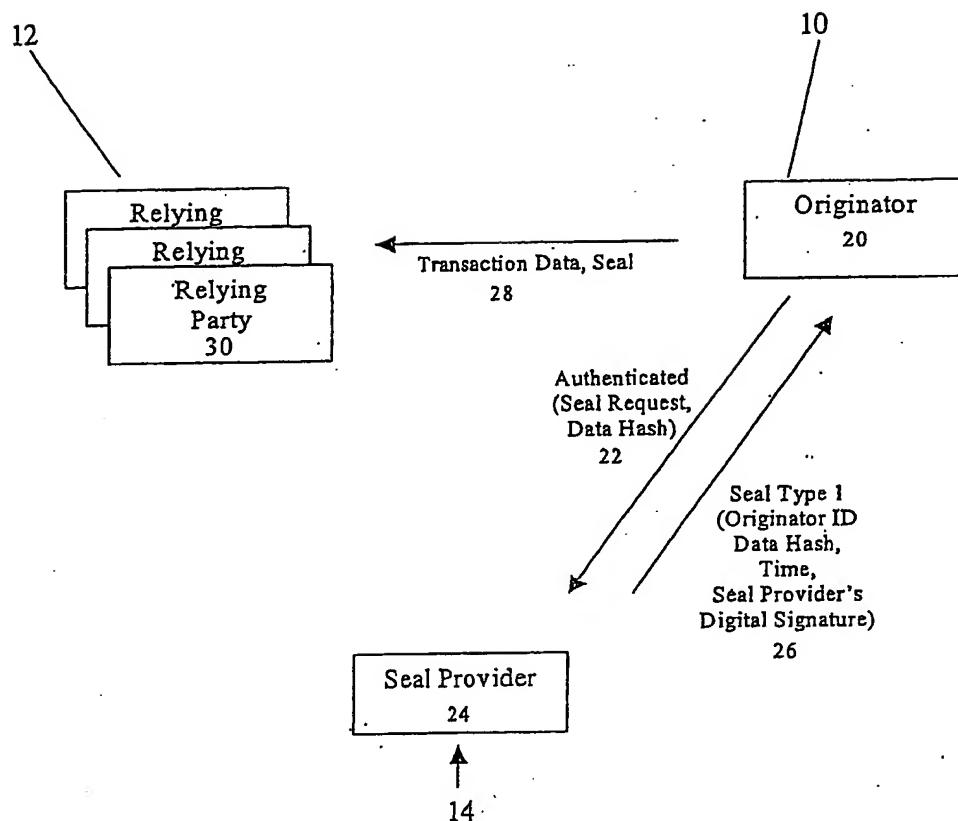


Figure 1

2/11

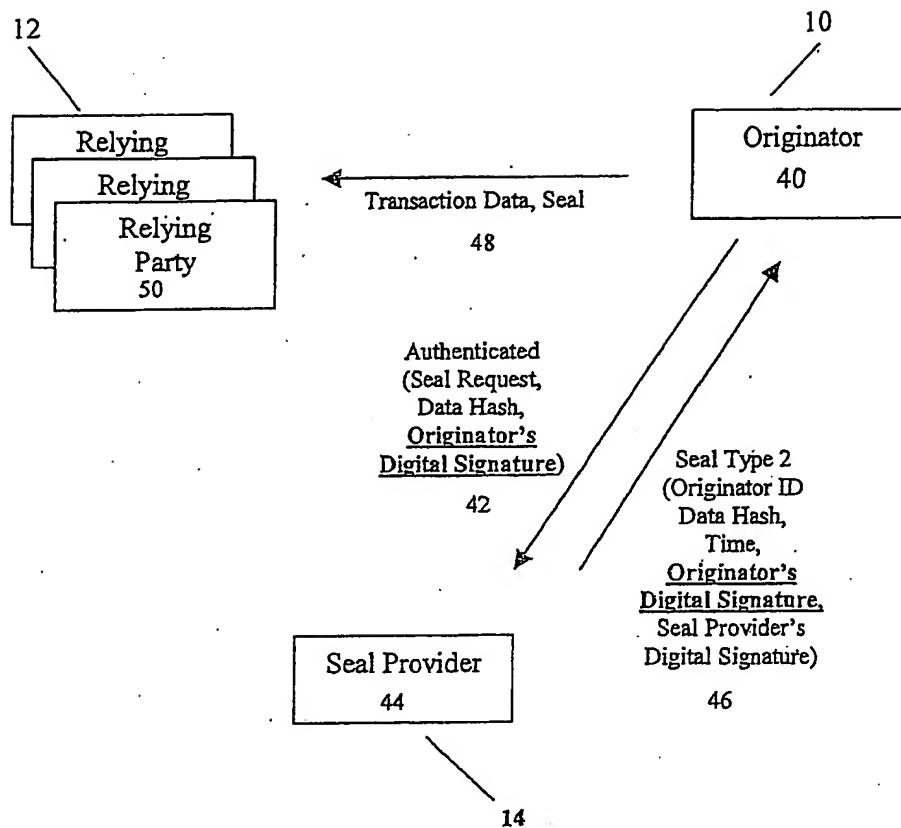


Figure 2 a

3/11

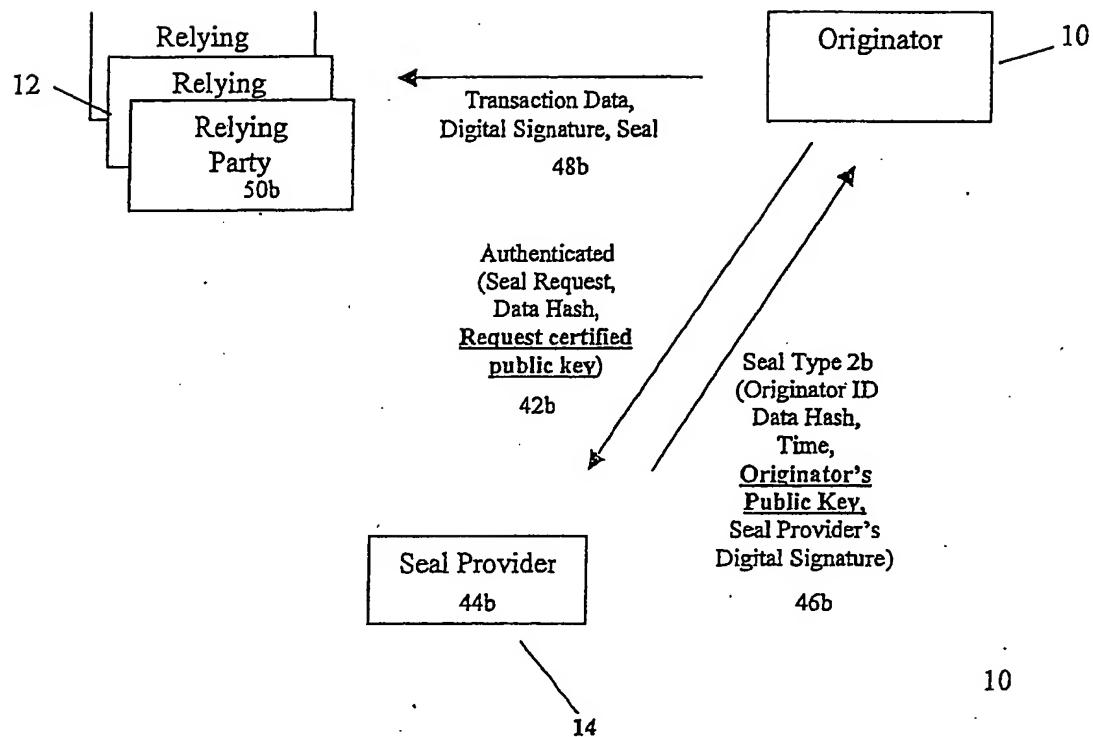


Figure 2b

4/11

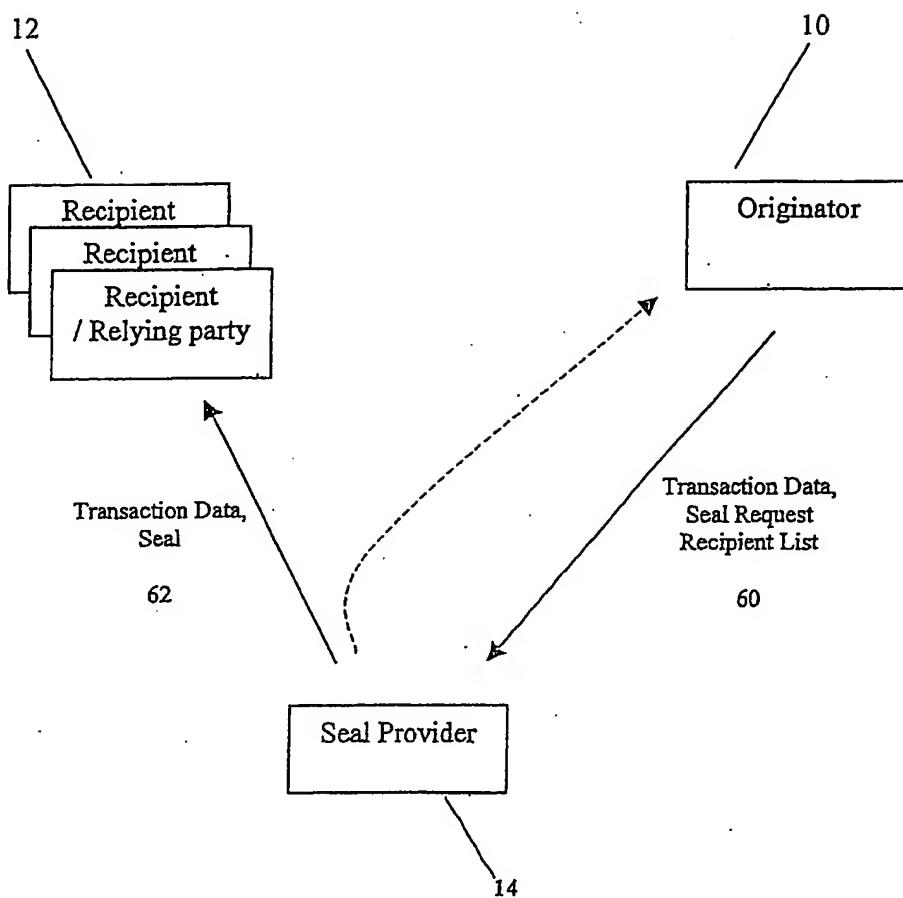


Figure 3

5/11

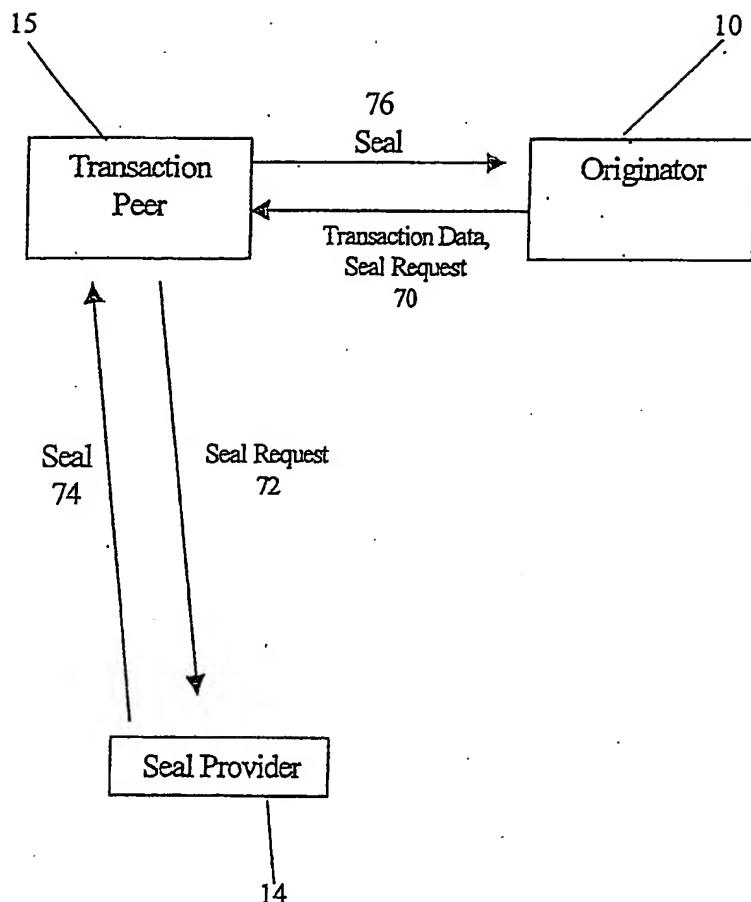


Figure 4

6/11

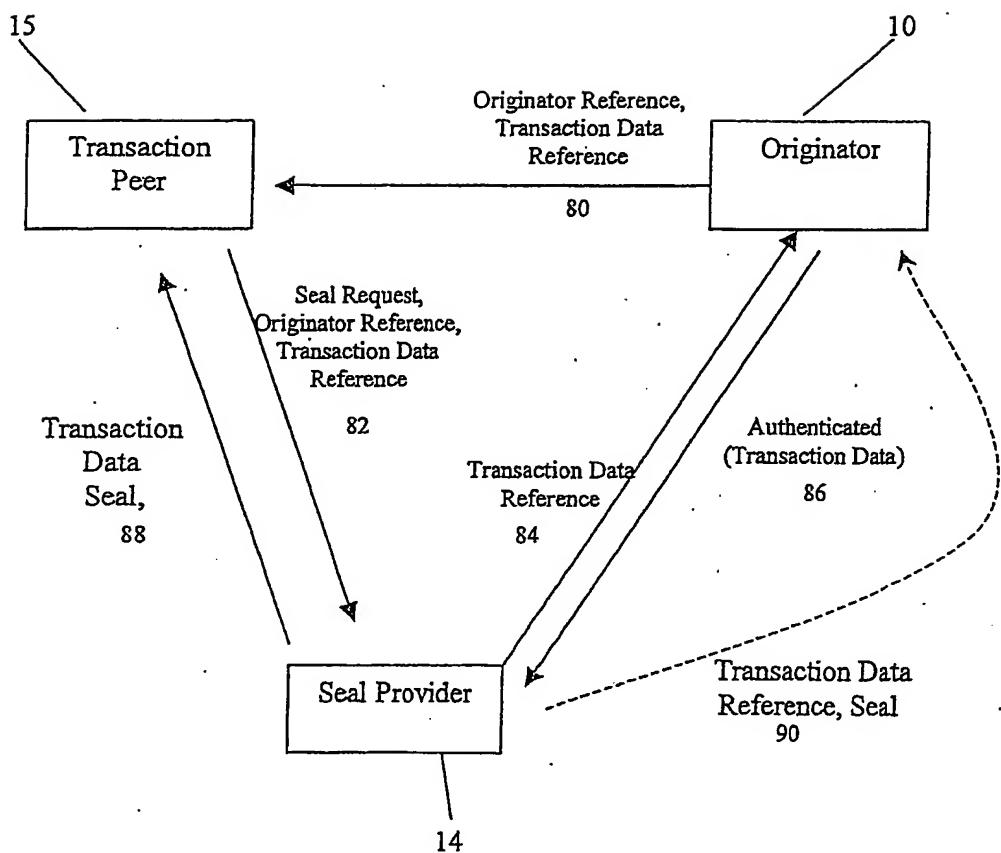


Figure 5

7/11

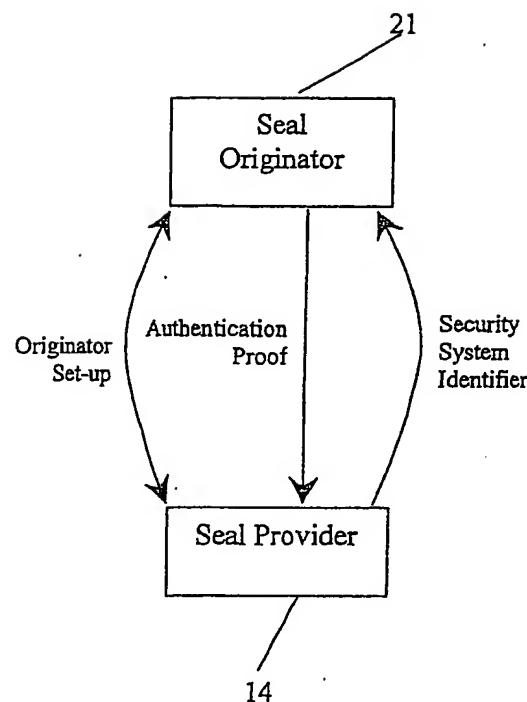


Figure 6

8/11

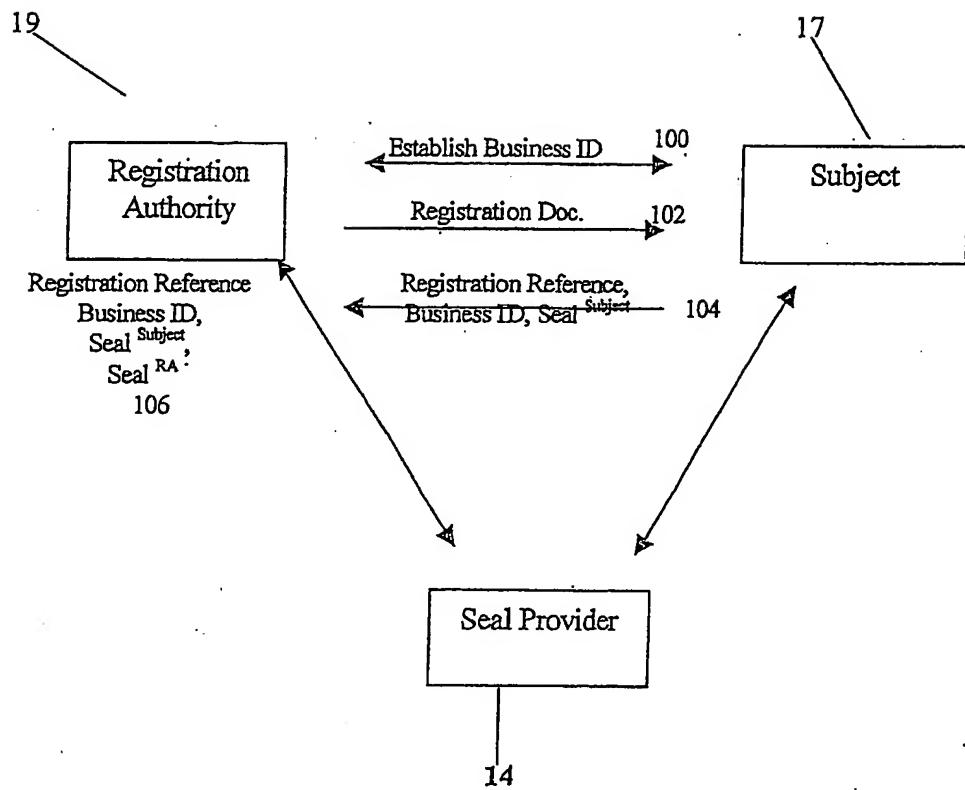


Figure 7

9/11

GrowlTech: Receipt & Record - Transaction Seal (1)
Sealed by SecurityAndStandards on behalf of
Secstan Test (User ID:1) of
R&R Test Community .1 (Community ID:1)
Sealed on: 16/12/2002 18:56:24.766 UTC

Seal
Header

MII CyQYJKoZIhvcNAQcCoIICu{jCCArYCAQMxCzAJBgUrDgMC
GjUAMIHSBgsqhkiG9w0BCRABBKCBwgSBvzCBvAIBAQYKKwYB
BAGEWQoDATAfMAcGBSsOAwIaBBQKrsVSjbMSmAPGrWNhzXBa
bjpD+QIEADtE+xgIMjAwMjEyMTYxODU2MjQuNzY2NjAKAgEA
gAIB9IEBAAEB/wIGNIaADBAoFikVjBUMQswCQYDVQQGEwJV
SzEdMBsGA1UEChMUU2VjdXJpdH1BbmRTdGFuZGFyZHMxDjAM
BgNVBAsTBVRTQS4zMRYwFAYDVQQDEw1TRUNTVEFOLjAwMDAx
MYIBzTCCAckCAQEWsjBFMQswCQYDVQQGEwJVUzERMA8GA1UE

Base64 encoded
Binary
Seal Protection
Data

Figure 8

10/11

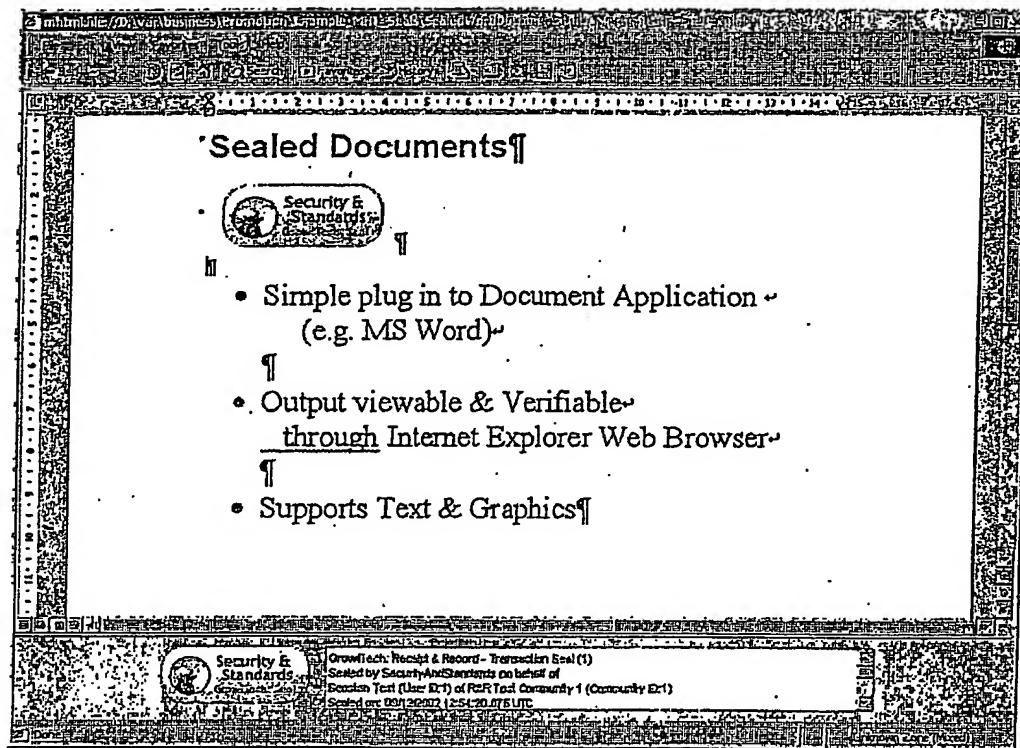


Figure 9

11/11

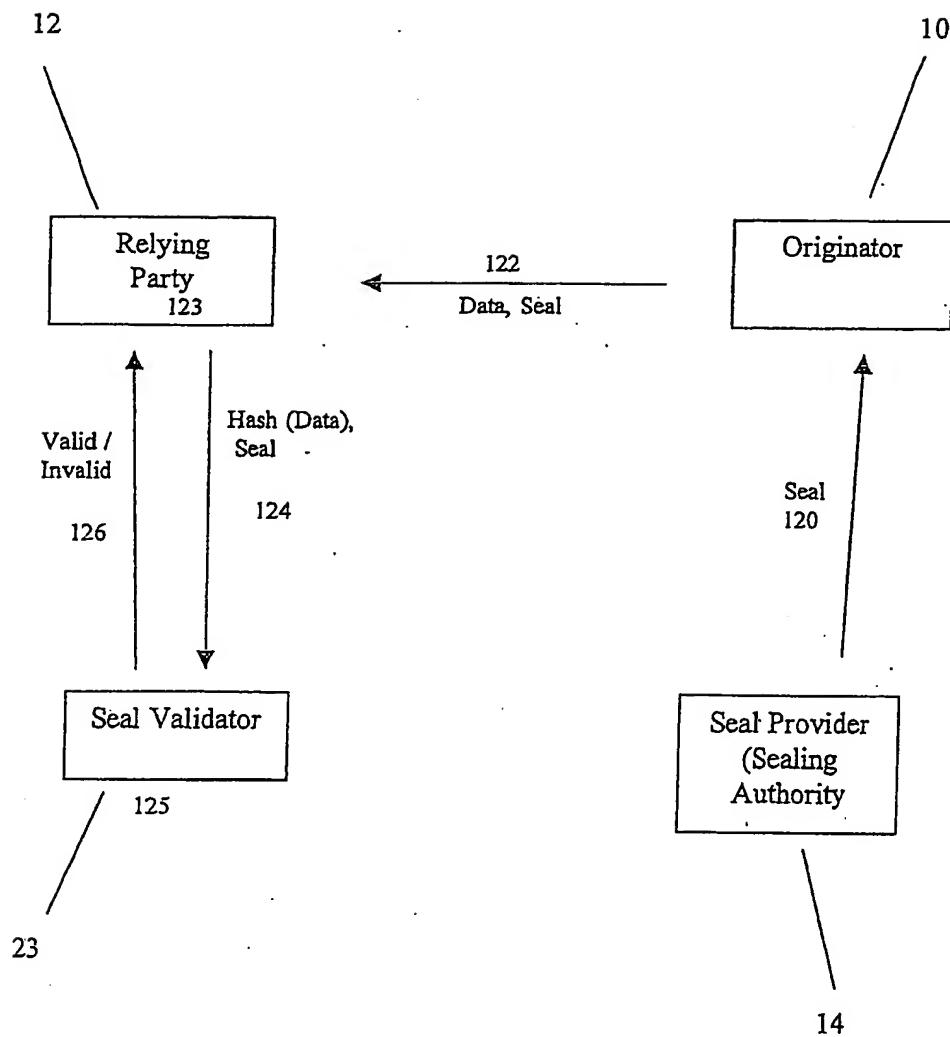


Figure 10

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB 03/03243

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L12/58 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the International search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	ZIXMAIL: "Zixmail technology" INTERNET CITATION, 'Online' 6 September 2000 (2000-09-06), XP002260773 Retrieved from the Internet: <URL: http://www.zixmail.com/zixmail.pdf> 'retrieved on 2003-11-07! the whole document	1-25
X	US 2002/032865 A1 (CHOU CHENG-FU ET AL) 14 March 2002 (2002-03-14) abstract paragraph '0061! - paragraph '0065!; figures 4, 5	1-25

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the International filing date
- *L* document which may throw doubts on priority, claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the International filing date but later than the priority date claimed

T later document published after the International filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

& document member of the same patent family

Date of the actual completion of the International search

Date of mailing of the International search report

27 November 2003

12/12/2003

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-3016

Authorized officer

Bertolissi, E

INTERNATIONAL SEARCH REPORT

Internat^k plication No
PCT/GB 03/03243

C(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/078355 A1 (SAMAR VIPIN) 20 June 2002 (2002-06-20) abstract paragraph '0044! - paragraph '0050! figures 1,2	1-25
P,X	US 2002/143710 A1 (LIU GARY) 3 October 2002 (2002-10-03) paragraph '0069! - paragraph '0090!; figures 3,4A,4B	1-25
A	US 6 393 566 B1 (LEVINE JUDAH) 21 May 2002 (2002-05-21) abstract column 2, line 8 -column 3, line 3; figures 1-5	1-25
A	WO 99 35785 A (KONINKL PHILIPS ELECTRONICS NV ;PHILIPS SVENSKA AB (SE)) 15 July 1999 (1999-07-15) abstract	1-25
A	PATENT ABSTRACTS OF JAPAN vol. 013, no. 477 (M-885), 27 October 1989 (1989-10-27) -& JP 01 188322 A (TOYOBO CO LTD;OTHERS: 01), 27 July 1989 (1989-07-27) abstract	1-25

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internat	Application No
PCT/GB	03/03243

Patent document cited in search report		Publication date		Patent family member(s)		Publication date
US 2002032865	A1	14-03-2002	NONE			
US 2002078355	A1	20-06-2002	AU CA WO	3662202 A 2426828 A1 0248848 A2	24-06-2002 20-06-2002 20-06-2002	
US 2002143710	A1	03-10-2002	NONE			
US 6393566	B1	21-05-2002	NONE			
WO 9935785	A	15-07-1999	US CN EP WO JP	6601172 B1 1254464 T 0963637 A2 9935785 A2 2001515612 T	29-07-2003 24-05-2000 15-12-1999 15-07-1999 18-09-2001	
JP 01188322	A	27-07-1989	JP JP	2108598 C 7106599 B	21-11-1996 15-11-1995	